AO 120 (Rev. 2/99)

TO: Mail Stop 8 Director of the U.S. Patent & Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450 E-filing	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Northern District of California on the following X Patents or ☐ Trademarks:

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
CV 07-03257 BZ	6/20/07	Northern District of California
PLAINTIFF		DEFENDANT
PRIVASYS INC		VISA INTERNATIONAL

SOLICITOR JUN 29 2007 U.S. PATENT & TRADEMARK OFFICE

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	7,195,154		(See attached Complaint)
2			
3			
4			
5			

In the above—entitled case, the following patent(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE
Richard W. Wieking	Simone Voltz	June 22, 2007

Copy 1—Upon initiation of action, mail this copy to Commissioner Copy 3—Upon termination of action, mail this copy to Commissioner
Copy 2—Upon filing document adding patent(s), mail this copy to Commissioner Copy 4—Case file copy

COUNT I
(Patent Infringement)

26. Visa has, without authority, consent, right or license, and in direct infringement of the Routhenstein Patent, made, used, offered for sale and/or sold products using the methods claimed in the patent in this country. This conduct constitutes infringement under 35 U.S.C. § 271(a).

27. In addition, Visa has in this country, through its promotion of Visa payWave (and similar brand names) and agreements with its issuing banks to distribute Visa payWave devices and to process transaction initiated from those devices, Visa has actively induced others to make, use, and/or sell the systems, products and methods claimed in one or more claims of the Routhenstein Patent. This conduct constitutes infringement under 35 U.S.C. § 271(b).

28. Visa's infringing conduct is unlawful and willful and will continue unless enjoined by this Court. Visa's willful conduct makes this an exceptional case as provided in 35 U.S.C. § 285.

29. As a result of Visa's infringement, Plaintiff has been damaged, and will continue to be damaged, until Visa is enjoined from further acts of infringement.

30. Plaintiffs face real, substantial and irreparable damage and injury of a continuing nature from Visa's infringement for which Plaintiff has no adequate remedy at law.

WHEREFORE, Plaintiff prays:

(a) That this Court find Visa has committed acts of patent infringement under the Patent Act, 35 U.S.C. § 271;

(b) That this Court enter judgment that:

(i) the Routhenstein Patent is valid and enforceable and;

(ii) Visa has willfully infringed the Routhenstein Patent;

(c) That this Court issue an injunction enjoining Visa, its officers, agents, servants, employees and attorneys, and any other person in active concert or participation with them, from continuing the acts herein complained of, and more particularly, that Visa and such other persons be permanently enjoined and restrained from further infringing the Routhenstein Patent;

(d) That this Court require Visa to file with this Court, within thirty (30) days after entry of final judgment, a written statement under oath setting forth in detail the manner in which Visa has complied with the injunction;

(e) That this Court award Plaintiff the damages to which it is entitled due to Visa's patent infringement, with both pre-judgment and post-judgment interest;

(f) That Visa's infringement of the Routhenstein Patent be adjudged willful and that the damages to Plaintiff be increased by three times the amount found or assessed pursuant to 35 U.S.C. § 284;

(g) That this be adjudged an exceptional case and that Plaintiff be awarded its attorney's fees in this action pursuant to 35 U.S.C. § 285;

(h) That this Court award Plaintiff its costs and disbursements in this civil action, including reasonable attorney's fees; and

(j) That this Court grant Plaintiff such other and further relief, in law or in equity, both general and special, to which it may be entitled.

DEMAND FOR JURY TRIAL

Plaintiff, by its undersigned attorneys, demands a trial by jury on all issues so triable.

Dated: June 20, 2007

Respectfully submitted,

SPENCER HOSIE (CA Bar No. 101777)
shosie@hosielaw.com
BRUCE WECKER (CA Bar No. 078530)
bwecker@hosielaw.com
HOSIE McARTHUR LLP
One Market, 22nd Floor
San Francisco, CA 94105
(415) 247-6000 Tel.
(415) 247-6001 Fax

ROBERT J. YORIO (CA Bar No. 93178)
CARR & FERRELL LLP
2200 Geng Road
Palo Alto, CA 94303
(650) 812-3400 Tel.
(650) 812-3444 Fax

Attorneys for Plaintiff
PRIVASYS, INC.

DISCLOSURE OF NON-PARTY INTERESTED ENTITIES OR PERSONS

Pursuant to Civil L.R. 3-16, Plaintiff, by its undersigned attorneys, certifies that as of this date, there is no such interest to report.

Dated: June 20, 2007

Respectfully submitted,

SPENCER HOSIE (CA Bar No. 101777)
shosie@hosielaw.com
BRUCE WECKER (CA Bar No. 078530)
bwecker@hosielaw.com
HOSIE McARTHUR LLP
One Market, 22nd Floor
San Francisco, CA 94105
(415) 247-6000 Tel.
(415) 247-6001 Fax

ROBERT J. YORIO (CA Bar No. 93178)
CARR & FERRELL LLP
2200 Geng Road
Palo Alto, CA 94303
(650) 812-3400 Tel.
(650) 812-3444 Fax

Attorneys for Plaintiff
PRIVASYS, INC.

SPENCER HOSIE (CA Bar No. 101777)
shosie@hosielaw.com
BRUCE WECKER (CA Bar No. 078530)
bwecker@hosielaw.com
HOSIE McARTHUR LLP
One Market, 22nd Floor
San Francisco, CA 94105
(415) 247-6000 Tel.
(415) 247-6001 Fax

ROBERT J. YORIO (CA Bar No. 93178)
CARR & FERRELL LLP
2200 Geng Road
Palo Alto, CA 94303
(650) 812-3400 Tel.
(650) 812-3444 Fax

Attorneys for Plaintiff
PRIVASYS, INC.

BZ

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA (SAN FRANCISCO)

PRIVASYS, INC,

Plaintiff,

v.

VISA INTERNATIONAL SERVICE ASSOCIATION, VISA U.S.A.,

Defendants.

C 07 3257

Case No. _____

ORIGINAL COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff PrivaSys, Inc. ("PrivaSys" or "Plaintiff") hereby files its complaint against Defendants Visa International Service Association and Visa, U.S.A. ("Visa" or "Defendants") for patent infringement. In support of its complaint, Plaintiff alleges as follows:

PARTIES

1. PrivaSys is a Delaware corporation, with its principal place of business in Newbury Park, California. PrivaSys is the assignee of the patent at issue in this case.

2. Defendants Visa U.S.A. and Visa International Service Association ("Visa International") are associations of independent banks and financial institutions and are structured as membership corporations. Defendants Visa U.S.A. and Visa International are organized under the laws of the State of Delaware, and each has its principal place of business in Foster City, California. Although Visa International has delegated certain authority to regional boards, including the Board of Directors of Visa U.S.A., Visa International retains ultimate authority over the policies and practices of Visa U.S.A., even for matters solely within the United States. Visa U.S.A., Visa International, and all of their respective predecessors and subsidiaries are referred to collectively herein as "Visa."

JURISDICTION AND VENUE

3. This complaint asserts a cause of action for patent infringement under the Patent Act, 35 U.S.C. § 271. This Court has subject matter jurisdiction over this matter by virtue of 28 U.S.C. § 1338(a). Venue is proper in this Court by virtue of 28 U.S.C. § 1391(b) and (c) and 28 U.S.C. § 1400(b).

4. This Court has personal jurisdiction over Visa because it provides infringing products and services in the Northern District of California and Visa has a regular and established place of business in this district.

INTRADISTRICT ASSIGNMENT

5. Pursuant to Civil LR 3-2(c), this case should be subject to district-wide assignment because it is an Intellectual Property Action.

BACKGROUND

The Pervasive Payment Card Fraud Problem

6. For the past 40 years, payment cards have been inanimate pieces of plastic. Each card has a primary account number in embossed characters, information about the cardholder also embossed, an encoded magnetic stripe ("magstripe") on the back of the card, and a printed and visible three or four digit security code.

7. The magstripe contains data that can be read by magstripe readers, the terminals used by merchants at the point of sale ("POS"). When a merchant swipes a card, a magnetic head reads the encoded data and then transmits the data to the issuing bank with an authorization request. "Track 1" data on the magstripe typically contains the customer's name, account number, expiration date, and a "discretionary data" field to be used by the issuing bank. "Track 2" data contains the account number, expiration date, and another "discretionary data" field, all of which must fit within approximately 40 digits of space.

8. A person who obtains the Track 1 and Track 2 account information and the printed security code has all the information that he needs to manufacture a counterfeit card. An increasing form of fraud consists of collecting valid account numbers, either through "skimming" (*e.g.*, collecting card numbers electronically) or through data compromise (e.g., computer hacking) and then using the account numbers and printed security code to

manufacture counterfeit cards. Payment card fraud using such techniques costs the issuing banks – and ultimately the cardholders – many billions of dollars a year.

9. Payment card fraud is being addressed in Europe and in Asia, in part, through the adoption of "smart cards." A smart card is a payment card equipped with a secure chip, possessing internal data processing functionality. Smart cards are more difficult to duplicate than conventional cards, and they have intrinsic security protection. In Europe, MasterCard and Visa have advanced smart cards through a joint venture known as EMVCo. ("EMV").

10. While smart cards offer many benefits, they cannot be read by conventional magstripe POS terminal readers. Instead, smart cards require new, more sophisticated terminals. In essence, full smart card adoption requires wholesale replacement of the existing POS magstripe terminals. This "re-terminalization" is expensive but essential to widespread smart card adoption.

11. MasterCard and Visa accelerated smart card adoption in Europe through what is known as "liability shift." In the United States, a POS merchant is not liable for loss when a fraudulent card is used in a "card present" transaction, so long as he properly obtains a "personal identification number" ("PIN") or a signature and obtains issuer authorization. Instead, the issuing bank absorbs that loss. Conversely, in countries that mandate the issuing banks release smart cards, a POS merchant in Europe bears the fraud loss unless he has invested in a smart card terminal, even if he innocently accepts a fraudulent card. Shifting the fraud loss to the merchant gives the merchant a strong incentive to invest in new smart card terminals.

12. MasterCard and Visa have been unable to introduce smart cards in the United States. In considerable part, this is due to the enormous cost of re-terminalization, estimated to be in the vicinity of $12-13 billion. Because MasterCard and Visa have been unable to

shift the fraud loss to POS merchants, those merchants lack the economic incentive to invest in new smart card terminals and have generally declined to do so.

13. Visa and MasterCard studied the business case for smart cards and concluded that widespread smart card adoption was not economically warranted in the United States, given the cost of re-terminalization, merchant resistance, and the expensive changes required in the issuing banks' back-office operations. Neither Visa nor MasterCard was able to break this technological logjam. As a result, the American payment card market did not respond to increasing multibillion-dollar skimming fraud through the widespread adoption of smart cards.

PrivaSys' Solution To Payment Card Fraud

14. PrivaSys was founded to develop innovative ways to reduce payment card fraud while working within the existing legacy system of magstripe readers and transaction networks. PrivaSys understood that smart cards would be adopted slowly if at all in this country, which gave rise to a compelling need to make the legacy system itself more secure. Prior security approaches, *e.g.*, card holograms or printed security codes, were easily circumvented, as they were static and unchanging. Thus, PrivaSys invented a new approach that would allow the card itself to become the center of innovation. Re-terminalization is unnecessary because data is received from the card in the traditional magnetic stripe data packet format.

15. The PrivaSys system creates an authentication code that is unique to each card and each transaction. The data are transmitted to the magstripe reader by a signal from the card. Because a counterfeit card lacks the ability to generate this unique code, or watermark, the issuing bank knows to reject the fraudulent transaction.

16. The PrivaSys method works as follows:

- Each card securely stores a card-specific, cryptographic key on a chip.
- Each card contains a "counter" that increments with every use or attempted use of the card.
- Each card contains a cryptographic algorithm, to calculate an authentication code.
- The information is processed through a triple-DES (or 3DES) encryption algorithm. The output of this algorithm is reduced to several digits unique to the specific transaction for the given card.
- These digits are referred to as a "dynamic authentication code" (or DAC). The DAC is placed in the discretionary data field of Track 1 and/or Track 2. The DAC is then communicated along with the account number, expiration date and a request for authorization to the issuing bank, all through the existing legacy infrastructure.
- The issuing bank has backend software that reproduces the DAC computation on a per-card, per-transaction basis. When the issuing bank receives an authorization request and accompanying DAC, it computes its own DAC for that card using that card's specific cryptographic key. It then compares its issuer-generated DAC to the card-generated DAC, and approves the transaction if the two match, and the other account information appears proper.

A counterfeit card does not have the ability to create the unique, transaction-specific DAC. In this way, the PrivaSys method detects the use of counterfeit cards and denies any transaction attempted, and does so within the existing magstripe legacy system.

17. PrivaSys' fraud prevention technology is not, however, limited to the legacy magstripe reader system. PrivaSys designed it to be adaptable to a variety of communications systems and transmission means– including radio frequency (RF), mobile (cellular wireless), IR (infrared) and broadcasted magnetic stripe systems.

18. PrivaSys' technology is designed to bridge the gap between traditional credit cards and fully EMV-compliant smart cards. Because it does not require full re-terminalization, PrivaSys reasonably believed that its technology would be adopted quickly,

populating the United States market with intelligent cards and payment devices. This would facilitate the ultimate transition to smart cards.

The PrivaSys Patent

19. Plaintiff owns a patent, U.S. Patent No. 7,195,154 ("'154"), issued on March 27, 2007, to inventor Larry Routhenstein covering PrivaSys' methods for providing secure transactions between a money source (such as a Visa issuing bank) and its customer credit or debit card holders. A true and correct copy of the '154 Patent is attached as Exhibit "A." Plaintiff is the legal and rightful owners of the Routhenstein Patent.

20. The '154 Patent contains thirty-five (35) patent claims covering a unique and novel method for generating and validating a dynamic code with each transaction transmitted over the existing payment card networks. In general, the patent discloses a method that uses an encrypted and compressed authentication code that is dynamically calculated with each transaction and transmitted via the discretionary data field through the legacy payment card processing system and which was validated by duplicating the calculation in the issuing bank's data processing systems and comparing two values for a match.

21. PrivaSys has licensed this technology to a number of Visa's principal competitors in contactless payment card and transaction processing businesses, including MasterCard and transaction processor First Data, Inc. Visa, however, has refused to take a license.

Visa's Infringing Services

22. Plaintiff's patent application was publicly known as early as March 27, 2003, when the application was published by the Patent Office. On the issuance of the patent, Visa became aware of it through ongoing licensing discussions among counsel. Despite this

knowledge, Visa has proceeded on a path of selling infringing products and services as detailed below.

23. Recently, Visa began to offer contactless cards or devices, *i.e.*, payment cards that do not need to be swiped through a magnetic reader, called variously "Visa Contactless," "Visa Wave," and Visa "payWave." These devices contain a small computer chip and a radio-frequency antenna (RF) that allows a reader to receive data from the device when it is placed in proximity to the reader (typically within a few centimeters). Visa's contactless devices are designed to send standardized magnetic stripe Track 1 or Track 2 data streams, *i.e.*, data is packaged as per the existing magnetic stripe legacy system protocols.

24. Visa's contactless payment protocols operate as follows: (1) there is a unique cryptographic key for each Visa payment device, be it a FOB or credit card; (2) the device generates a unique several digit cryptogram for each and every card-specific transaction; Visa refers to this unique cryptogram, or watermark, as the dynamic Card Verification Value or "dCVV". The dCVV is packaged as per existing magnetic stripe data protocols and sent in the discretionary data field through the existing legacy system; (3) Visa provides the specifications for the de-encryption engine for dCVV de-encryption to the issuing banks, those banks maintain a backend de-encryption engine as specified by Visa, which replicates the dCVV calculation for each card-specific use, and approves the transaction if the dCVVs match and the other account data appear proper.

25. The use of a dynamic cryptogram is essential to the success of the Visa Wave product. Absent such a cryptogram, the RF transactions could be easily skimmed or breached, and fraud would proliferate.